AMENDMENTS TO CLAIMS

Claims 1 - 82 (cancelled)

Claim 83 (currently amended): A system for secure transmission of protected content, the system comprising:

a head-end operative to send entitlement information controlling access to the protected content;

a security server;

a plurality of recipient modules comprising:

a first plurality of security-element recipient modules; and

a second plurality of non-security-element recipient modules, said first plurality of security-element recipient modules differing from said second plurality of non-security-element recipient modules in that each of said first plurality of security-element recipient modules includes a smart card operative to process the entitlement information received from the head-end and to produce therefrom a key for accessing the protected content; and

a secure communication channel for supporting communication between said security server and at least one of said plurality of recipient modules, wherein

the head-end sends the entitlement information both to the security server and to at least some of the plurality of recipient modules~~; and~~

~~said plurality of recipient modules comprises:~~

~~a first plurality of security-element recipient modules; and~~

~~a second plurality of non-security-element recipient modules, the first plurality of recipient modules differing from said second plurality of recipient modules in that each of the first plurality of security-element recipient modules includes a renewable security element operative to process the entitlement information received from the head-end and produce therefrom a key for accessing the protected content~~, and

in a first mode of operation, at least one of the second plurality of non-security-element recipient modules receives a first key in a multiple key hierarchy via said secure communication channel, and

in a second mode of operation, said at least one of the non-security-element recipient modules receives the protected content and an encrypted key, said encrypted key being a second key in said multiple key hierarchy, said at least one of the non-security-element recipient modules being operative to utilize the first key to decrypt the encrypted key to form a decrypted key, said at least one of the non-security-element recipient modules only being capable of accessing the protected content with said decrypted key, and

said first key and said second key are prepared by said security server based, at least in part, on the entitlement information sent by the head-end.

Claim 84 (previously presented): The system according to claim 83, wherein said first key is contained in a VEMM, said VEMM further comprising an access criteria reference for determining whether said at least one of the non-security-element recipient modules is entitled to access the protected content, said VEMM being prepared by said security server based, at least in part, on the entitlement information sent by the head-end.

Claim 85 (previously presented): The system according to claim 84 and wherein said VEMM is sent upon request by said at least one of the non-security-element recipient modules.

Claim 86 (previously presented): The system according to claim 85 and wherein said request includes an access criteria reference.

Claim 87 (previously presented): The system according to claim 85 and wherein said request is initiated in response to an impulse pay per view (IPPV) request by a user.

Claim 88 (previously presented): The system according to claim 84, wherein said access criteria reference for each item of protected content is associated with a separate access key.

Claim 89 (previously presented): The system according to claim 84, wherein said encrypted key further comprises an encrypted control word.

Claim 90 (previously presented): The system according to claim 89, wherein said encrypted control word is contained in a VECM, said VECM further comprising an access criteria reference for identifying said first key for decrypting said encrypted control word by said at least one of the non-security-element recipient modules, said VECM being prepared by said security server based, at least in part, on the entitlement information sent by the head-end.

Claim 91 (previously presented): The system according to claim 90, wherein said secure communication channel further comprises a subscriber key, such that said first key is encrypted with said subscriber key for being transmitted to said at least one of the non-security-element recipient modules, and such that said at least one of the non-security-element recipient modules is capable of decrypting said subscriber key.

Claim 92 (previously presented): The system according to claim 90, wherein said secure communication channel comprises a second plurality of secure communication channels each associated with one of the second plurality of non-security-element recipient modules, and

each of the secure communication channels further comprises a subscriber key of the associated one of the non-security-element recipient modules, such that said first key is encrypted with said subscriber key for being transmitted to said one of the non-security-element recipient modules, and such that only said one of the non-security-element recipient modules is capable of decrypting said subscriber key.

Claim 93 (previously presented): The system according to claim 91, wherein said one of the non-security-element recipient modules further comprises a secret, said secret being required for decrypting said subscriber key, and said secret comprising a part of said secure communication channel.

Claim 94 (previously presented): The system according to claim 93, wherein said one of the non-security-element recipient modules comprises at least one permanent read-only storage medium for storing said secret.

Claim 95 (previously presented): The system according to claim 94, wherein said secret is permanently stored on said at least one permanent read-only storage medium during manufacture of said one of the non-security-element recipient modules.

Claim 96 (previously presented): The system according to claim 94, wherein said one of the non-security-element recipient modules comprises at least one generic chip, said at least one generic chip comprising said at least one permanent read-only storage medium for storing said secret.

Claim 97 (previously presented): The system according to claim 93, wherein said security server receives said subscriber key encrypted with said secret and an unencrypted subscriber key, but wherein said security server does not receive said secret.

Claim 98 (currently amended): The system according to claim 84, wherein said head-end sends [[a]] an Entitlement Management Message (EMM) to said security server, for providing said access criteria reference to said security server.

Claim 99 (currently amended): The system according to claim 98, wherein said head-end sends at least information for generating said control word to said security server in an Entitlement Control Message (ECM).

Claim 100 (previously presented): The system according to claim 99, wherein said head-end also sends said ECM to at least one of the security-element recipient modules.

Claim 101 (previously presented): The system according to claim 99, wherein a different VEMM is transmitted periodically.

Claim 102 (previously presented): The system according to claim 101, wherein a different VEMM is transmitted if said at least one of the non-security-element recipient modules is off-line for at least a predetermined period of time.

Claim 103 (previously presented): The system according to claim 99, wherein said VEMM is unicast to each of a subset of said plurality of recipient modules.

Claim 104 (previously presented): The system according to claim 99, wherein said security server comprises a remote renewable security element for storing said subscriber key and for providing said encrypted first key and said encrypted control word to said security server.

Claim 105 (previously presented): The system according to claim 104, wherein said subscriber key at said remote renewable security element is capable of being renewed.

Claim 106 (previously presented): The system according to claim 104, wherein said remote renewable security element further comprises a hardware component and a software component.

Claim 107 (previously presented): The system according to claim 106, wherein said software component determines one or more entitlements for permitting said VEMM to be generated for said at least one of the non-security-element recipient modules.

Claim 108 (previously presented): The system according to claim 106, wherein said hardware component encrypts said access key and said control word.

Claim 109 (previously presented): The system according to claim 104, further comprising a plurality of said remote renewable security elements, and further comprising a broadcaster of the protected content for controlling said plurality of said remote renewable security elements.

Claim 110 (previously presented): The system according to claim 104, wherein a plurality of said remote renewable security elements is controlled by said security server.

Claim 111 (previously presented): The system according to claim 110, wherein said security server and said plurality of said remote renewable security elements share a server key for at least decrypting at least said access key.

Claim 112 (previously presented): The system according to claim 111, wherein said security server generates said access key in an encrypted form as an encrypted access key, and wherein said remote renewable security element decrypts said encrypted access key to form said access key according to said server key.

Claim 113 (previously presented): The system according to claim 104, wherein at least some of said plurality of recipient modules each comprise a set-top box.

Claim 114 (previously presented): The system according to claim 83 and wherein at least one of said security server and said secure communication channel is implemented with redundant components.

Claim 115 (previously presented): The system according to claim 83 and wherein the server comprises:

(a) a remote renewable security element;

(b) an entitlement message generator; and

(c) a control word message generator, and

the protected content is broadcast by the head-end, the head-end providing an access criteria reference and a control word for accessing the protected content, and

said entitlement message generator receives the access criteria reference from the head-end and queries said remote renewable security element to determine whether the at least one of the non-security-element recipient modules is entitled to receive the protected content, such that if the at least one of the non-security-element recipient modules is entitled to receive the protected content, said entitlement message generator generates a VEMM comprising an encrypted access key and the access criteria reference, and

if the at least one of the non-security-element recipient modules is entitled to receive the protected content, said control word message generator receives the control word from the head-end and generates a VECM comprising an encrypted control word, such that the at least one of the non-security-element recipient modules cannot access the protected content without said VEMM and said VECM.

Claim 116 (previously presented): The system according to claim 83 and wherein the server comprises:

(a) a remote renewable security element for determining whether the at least one of the non-security-element recipient modules has at least one entitlement to the protected content;

(b) a VEMM generator for generating a first message containing a first key, said VEMM generator only generating said first message if the at least one of the non-security-element recipient modules has said at least one entitlement; and

(c) a VECM generator for generating a second message containing a second key, said second key being encrypted with said first key, wherein the protected content is only accessible according to said second key.

Claim 117 (cancelled)